IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

A Study of Cyberthreats and Cybersecurity in Online Gaming

Ms. Tanvi Thakkar
Research Scholar, Department of Law, DACN, Nagpur, India
tnv_thakkar@yahoo.co.in

Abstract: *Online gaming industry has witnessed a wide and a rapid growth in India and worldwide over the recent years. The way the gamers play games has evolved over a period of time beginning from board games, card games etc. to playing of games online with use of internet. The online games enable players from different geographies to connect, collaborate, and socialize while playing games through the medium of internet.*

In today's times when the online gaming is booming, it involves huge amounts of money. Apart from the finances, online gaming industry is sitting on a heap of data. It involves vast amount of data exchanges including personally identifiable data of the players, banking details so on and so forth. With this the online gaming industry being more lucrative and profitable than ever is not spared by the cyber criminals. The online gaming attracts a number of cyberthreats, cyberattacks, financial frauds etc.At the back drop or to say the initiators of the online games are the online gaming businesses which offer varied arena of online games to the gamers' community. While the gaming industries collect the personal data of the players, they themselves are at risk of financial frauds and reputational damage.

Given the vulnerability and the risks involved, the gaming businesses shall invest in and implement right security controls which protect against the cyberthreats likely to be faced by the gamers and the businesses itself. These controls are nothing but cybersecurity systems and technologies which prevent data thefts, secure the transactions, ensure protection against cyber-attacks and the like.

The entire gamut of online gaming needs to be regulated and shall have a stringent legal protection in place. The current regulatory framework in India comprises of certain provisions which govern the data principals i.e. the players of online gaming and data fiduciaries i.e. the gaming businesses.

This paper will study the evolution the gaming industry, the cyberthreats faced or likely to be faced by the gaming industry, the cybersecurity systems which are imperative against the cyberthreats and the regulatory framework governing the cyberspace and cybersecurity of online gaming industry in India. The paper will also provide appropriate suggestions..

Keywords: Cyberthreats, cybersecurity, online gaming, online gaming regulations

I. INTRODUCTION

There's a game for every player and the online gaming has enabled more options. Online gaming can simply be defined as a game offered through the medium of internet and played by a gamer through an electronic device or an intermediary. The landscape of games has evolved over the years. In India, one can say that the online gaming began in the early 2000s,when middle income groups started to use console and computer games. Though the usage was limited, itmarked the potential of online gaming which was to come on a large scale in future in India. Later in mid-2000s, online gaming was introduced to various socio-economic groups through the advent of social media. The gamers began to learn and explore various games using the social media platforms. By 2015-16, smartphones penetrated the market backed by high-speed internet service providers, which boosted the online gaming market. The highest selling smartphones available at reasonable prices, possessing good quality graphics have become the new age entertainment and experience on the go for the online players community. The recent years when the pandemic took the world indoors, people turned to the digital mediums for entertainment which led to a surge in playing games online. The percentage of game downloads increased exponentially. With this, the revenues of the online gaming industries grew.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

Though the pandemic has subsided, the trend continues. The online gaming industry has witnessed a remarkable growth.

A rise of in a sector, comes with its own challenges, and the gaming industry is no exception.

The risks which online gaming is prone to includes cyber threats, cyber security concerns, cyber-attacks, financial frauds etc. Its not just the gamers who are falling prey to cyber threats but also the gaming industries who offer the online games to the gamers community face dangers like phishing, data breaches, money laundering, viruses so on and so forth.

With the increase in cyber threats, a need of having robust cyber security systems has emerged. Cyber security comprises of protecting of the devices like mobile phones, tables, computers and also securing digital networks such that the activities of the third parties or cyber-criminals are blocked from harming the users. The entire gamut of online gaming, consisting of the gamers, gaming industries, financial institutions, network providers, while offering the games online involve financial, personal and similar information, which shall be well safeguarded against all sorts of cyber threats and cyber-attacks.

The paper will study the fast-growing gaming industry and the behavioural patterns of the gamers community, will investigate the cyber threats likely to harm the online gaming and suggest cyber security measures which can be adopted by the gamers and the industry to curb the cyber threats. The paper also analyses the regulatory framework governing the cyber space captured by online gaming.

GAMING INDUSTRY AND THE GAMERS

"*India's gaming market grew 23 per cent year-on-year (Y-o-Y) by revenue to $3.8 billion in financial year 2023-24 (FY24), despite the newly imposed 28 per cent blanket goods and service tax (GST) on online gaming, according to a report by gaming-focused venture capital firm Lumikai.*

With sustained growth in in-app purchases and ad revenue, the gaming market is expected to cross $9.2 billion by FY29, growing at a five-year compound annual growth rate (CAGR) of 20 per cent, Lumikai's 'State of India Interactive Media and Gaming Research' said."[1]

The gaming sector, which was once a niche sector, now constitutes one of the fastest growing sectors. Gamers are shifting to playing games virtually, as it becomes easy for them to access the virtual world from anywhere and at any time. While some games yield monetary profits, which is lucrative enough, however it is also the recreational aspect which is attracting the gamers community. The online gaming provides a vibrant and graphic experience on the go.

In contract to the famous belief that online games are being played only by the children and teenagers, a large number of adults also play games online and indeed form a substantial part of the gamers. The industry is shaping up to be inclusive and collaborative and this is being witnessed world over.

"Currently, gaming constitutes 30 per cent of the broader $12.5 billion new media market, and is its fastest growing segment. The Indian gaming market added 23 million new gamers to cross 590 million total gamers in FY24. At the same time the average weekly time spent on games increased by 30 per cent, from 10 hours to 13 hours, the report said."[2]

CYBER THREATS OF ONLINE GAMING

"With the growth of the online gaming sector, cyberattacks have risen, with over 75 percent of Indian gamers reporting attacks on their account in a 2021 survey."[3]The online games are on radar of cybercriminals for cyberattacks. With the huge financial gain which the online gaming industry promises, the cyber attackers are constantlydeveloping new cyber

[1]https://www.business-standard.com/industry/news/gaming-market-to-grow-at-25-to-9-2-bn-by-fy29-despite-gst-burden-report-124111100496_1.html

[2]https://www.business-standard.com/industry/news/gaming-market-to-grow-at-25-to-9-2-bn-by-fy29-despite-gst-burden-report-124111100496_1.html

[3]Prateek Tripathi, "Cybersecurity Threats in Online Gaming: Learnings for India," ORF Issue Brief No. 684, Observer Research Foundation, January 2024

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

threats and hacks to breakdown this new gaming ecosystem. A few common cyberthreats and risk which the online gaming industry is likely to face are as follows:

Malware and viruses

The gamers in the wake of playing and saving on some money, download free or less expensive games, which are fake, unreal, and illegal. The downloading such games unknowingly, holds a high risk of viruses and malware getting downloaded along. Once viruses and malware are into the systems of the gamers, it has access to the personal data and information of the gamers, which can easily be stolen and misused.

Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) Attacks are attacks wherein hackers overload the traffic in online gaming leading to a crash which interrupts the gaming service accessible to the gamers. Such attacks prevent gamers admission to the gaming services and the downtime and the recovery period can become a costly affair for the online gaming service provider. Such breaks do not cause any harm to the data of the gamers, however it's just causes displeasure and irritation among the gamers.

Hacking and Cheating

Hacking is the most common and one of the major challenges faced by online gaming. Hacking involves account hacking or unauthorized access to a gamer's account to gain or steal gamer's information, game related assets or seize the account entirely.

Cheating is bit different than hacking. Cheating includes use of variousunauthorised tricks to gain an unfair advantage over the gamer in the online gaming. For instance, in multiplayer online games, a technique of "lag switching"is used, wherein one of the gamers purposely advances a lag in the game such that the other gamers earn an unfair advantage.

Phishing

Phishing attacks are in the form fake emails, links or sites, sent to the gamers while the game is on. These appear real, coming from the gaming service provider, asking to download or add bonus points or sign up on a page. Once clicked, it can install malware or virus in the gamers system which can be harmful and unsafe.

Identity theft

One of the options available in online gaming is chat. The cybercriminals use the chat function to have a conversation with the gamers and extract personally identifiable information, which in turn is used to develop profiles. The cybercriminal tactfully collects personal sensitive information like name, address, phone numbers etc. which is very unsafe and risky for the online gamers.

Cyber bullying

While playing games online, the gamers can be subject to bullying or abuse from the other gamers. The cyber criminals or to say the cyber bullies can very well manipulate the targets to revealing personally identifiable information, which can be later on used against the them.

Data Breaches

"The online gaming community will be an emerging hacker surface, with cybercriminals posing as gamers and gaining access to the computers and personal data of trusting players." ---- 2019 Experian Data breach industry forecast.[4]

In addition to the gamers, the online gaming service providers can also fall prey to cyber attacks and cyberthreats. The hackers can target the gaming service providers directly. In case successful, the hackers can rob a lot of information of data including gamers identity, monies earned and transacted, sources code so on and so forth.

[4]https://www.wipro.com/platforms-and-software-products/game-on-the-need-for-cybersecurity-in-gaming/

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

CYBERSECURITY

The frequent occurrences of the cyber threats and cyber-attacksemphasizes uponan urgent need for implementation of robust cyber security measures to safeguard the gaming services providers and the gamers as well. This has led to a surge in development of highest secured systems including fraud detection systems, in order to address the future inevitablemalicious cyber-attacks likely to be faced by the online gaming industry.

Here are a few measures which can be adopted to prevent the cyberattacks and cyberthreats from striking the online games:

· To create strong passwords. Different passwords shall be set for different portals and shall not repeated or reused.
· To avoid clicking/ accessing suspicious links.
· To facilitateMulti-Factor Authentication(MFA) for gaming accounts
· Use a secure and trustworthy anti-virus
· Download a reliable security software
· Keep the operating systems and software updated regularly
· Avoid and not access doubtful links or unverified apps
· Be attentive always while playing games and not give in to the extra bonusses or points for winning
· Use only trustworthy and official links to download games
· Shall not share any kind of personally identifiable information
· Be cautious of any form of unauthorised phishing attacks or lucrative offers
· Keep oneself updated on the latest cyber security measures

Furthermore, there are measures which the gaming service providers too, being the giants in the industry, must adopt in creating a safe gaming world and enabling a secure gaming experience for the gamers community.

In a world where cybercriminals are getting bolder (think a billion data records released on the dark web by a hacker, it's imperative that gaming companies invest in and make use of the right security controls. The industry should adopt cybersecurity in the entire lifecycle of game development and deployment along with the platforms on which these are used. High-level guidelines to achieve better security assurance:

Enable multi factor authentication to protect against identity theft
Comply with PCI DSS and institute safe online payments to protect financial information
Ensure confidentiality of databases to protect sensitive information from being disclosed to unauthorized parties
Put a stop to back date frauds
Ensure protection against DoS and DDoS attacks that disrupt gamer experience by breaking connectivity
Ensure that security is embedded in the entire lifecycle of game development, release campaigns, marketing etc.
Protect against in-game phishing that usually happens via the messaging feature within the games[5]

REGULATORY FRAMEWORK

In India, the regulatory framework varied in nature. There's no uniform law which governs the gamut of online gaming. Beginning with, there exists the Public Gambling Act of 1867, which governs the activities like gambling betting etc. However, its obvious that the law is from the pre-internet era and there fore lacks provisions governing online games.

Under the Constitution of India, gaming forms part of the state list, enabling states to regulate the subject in their respective state territories. This has laid to multi laws prevalent in the country.

The main governing law governing the sector is the Information Technology Act, 2000, which has in it certain provisions which can be generally applies in case of hacking, theft etc. occurring in the field of online gaming.

Recently, the Ministry of Electronics and Information Technology (MeitY) released draft rules for online games which provides for a few provisions as follows:

Online games have to be registered with Self Regulatory Body (SRB).
Following due diligence.
Random number generation certificate.
Restrictions on betting.

[5]https://www.wipro.com/platforms-and-software-products/game-on-the-need-for-cybersecurity-in-gaming/

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

Appointment of a compliance officer.

II. CONCLUSION

In India's gaming industry is booming at a fast paced. With the rise in the industry the cyber threats and attacks too are on rise. This needs to be addressed by strong and robust cyber security. The cyber security measures shall be adopted by both viz the gaming service providers and the gamers too. Together, the risks and challenges posed by the cyber threats and attacks can be curbed providing a safe and secure gaming environment.